DOC 55 **1251/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

13 mai 2020

PROPOSITION DE LOI

relative à l'utilisation d'applications numériques de traçage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population

(déposée par
Mme Kathleen Verhelst,
MM. Michael Freilich et Khalil Aouasti,
Mme Jessika Soors,
M. Gilles Vanden Burre,
Mme Nathalie Gilson,
MM. Sammy Mahdi et Kris Verduyckt,
et Mme Catherine Fonck)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

13 mei 2020

WETSVOORSTEL

betreffende het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking

(ingediend door
mevrouw Kathleen Verhelst,
de heren Michael Freilich en Khalil Aouasti,
mevrouw Jessika Soors,
de heer Gilles Vanden Burre,
mevrouw Nathalie Gilson,
de heren Sammy Mahdi en Kris Verduyckt
en mevrouw Catherine Fonck)

RÉSUMÉ

La présente proposition de loi vise à créer le cadre légal pour l'utilisation d'applications numériques de traçage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population, plus particulièrement en ce qui concerne les garanties en matière de la protection des données à caractère personnel auxquelles ces applications de traçage de contacts doivent satisfaire.

SAMENVATTING

Dit wetsvoorstel strekt ertoe een wettelijk kader te scheppen voor het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking, meer bepaald voor wat betreft de nodige waarborgen op het niveau van de bescherming van persoonsgegevens waaraan deze contactopsporingsapplicaties moeten voldoen.

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
cdH	:	*centre démocrate Humaniste*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

1. ***Contexte***

La pandémie COVID-19 met la Belgique devant un défi inouï sur le plan de nos soins de santé et le bien-être de notre société. Le fait de diminuer les restrictions sur les mouvements valables depuis le 18 mars 2020 doit se fonder sur une combinaison de mesures d'accompagnement et nécessitera également la confiance et la poursuite des efforts de l'ensemble de la population.

Une stratégie de sortie réussie nécessite en particulier de rompre la chaîne des contaminations. Les éléments suivants peuvent contribuer à cet effet:

1. d'un côté, tester de manière systématique et répétitive pour détecter les personnes contaminées. Les personnes contaminées sont ensuite encouragés à s'auto-isoler;

2. de l'autre côté, la détection des contacts des personnes contaminées. Ces contacts sont ensuite encouragés à leur tour de s'auto-isoler et ils pourront être testés.

Le traçage des contacts des personnes contaminées et le fait d'encourager ces contacts de prendre les mesures nécessaires est primordial pour éviter de nouveaux foyers de contamination, qui menacent la santé publique. Le traçage des contacts est possible de plusieurs façons. Les méthodes les plus évidentes sont le traçage des contacts manuels et numériques. Avec le traçage manuel on choisit par exemple la mise en place de call centers qui contactent une personne contaminée et essayent ensuite avec la personne concernée de retracer les éventuels contacts qui ont eu lieu. Les personnes de contact sont contactées à leur tour par le call center. Il est évident que l'application de cette méthode de traçage de contacts implique une interférence importante dans la vie privée de la personne concernée. De plus, l'efficacité est limitée, vu qu'il n'est pas toujours possible de se rappeler exactement avec qui on a eu des contacts pendant une certaine période de temps, encore moins d'avoir les données de contact de toutes ces personnes. Cela demande également du temps d'atteindre ces personnes de contact, ce qui fait qu'à leur tour elles ont pu contaminer d'autres personnes entre-temps.

L'utilisation de nouvelles technologies peut donc jouer un rôle primordial dans l'évolution de la pandémie

TOELICHTING

DAMES EN HEREN,

1. ***Context***

De COVID-19-pandemie plaatst België voor ongekende uitdagingen op het vlak van onze gezondheidszorg en het welzijn van onze samenleving. Het terugschroeven van de beperkingen op verplaatsingen die sinds 18 maart 2020 gelden moet berusten op een combinatie van begeleidende maatregelen en zal ook het vertrouwen en verdere inspanningen van de gehele bevolking noodzaken.

Een succesvolle exitstrategie vergt in het bijzonder dat de keten van besmettingen doorbroken wordt. De volgende elementen kunnen daartoe bijdragen:

1. enerzijds het systematisch en herhaald testen om besmette personen op te sporen. Besmette personen worden vervolgens aangespoord om in zelf-isolatie te gaan;

2. anderzijds het opsporen van de contacten van de besmette personen. Deze contacten worden vervolgens op hun beurt aangespoord om in zelfisolatie te gaan en kunnen worden getest.

Het opsporen van de contacten van besmette personen en het aansporen van deze contacten om de nodige maatregelen te nemen, is cruciaal om nieuwe besmettingshaarden, die de volksgezondheid bedreigen, te voorkomen. Contactopsporing kan op verschillende manieren gebeuren. De meest voor de hand liggende methoden zijn manuele en digitale contactopsporing. Bij manuele opsporing wordt geopteerd voor bijvoorbeeld het installeren van call centers die een besmette persoon opbellen en vervolgens met hem/haar mogelijke contacten die hebben plaatsgevonden samen trachten te achterhalen. De contactpersonen worden dan op hun beurt gecontacteerd door het call center. Het spreekt voor zich dat de toepassing van deze methode van contactopsporing een belangrijke inmenging in de persoonlijke levenssfeer van de betrokkenen vormt. Bovendien zijn er ook beperkingen wat betreft de doeltreffendheid aangezien het niet altijd mogelijk is om zich exact te herinneren met wie men allemaal contact heeft gehad over een bepaalde tijdsperiode, laat staan dat men van al die personen de contactgegevens zou hebben. Het vergt ook tijd om de contactpersonen te bereiken waardoor zij intussen opnieuw andere personen kunnen hebben besmet.

Het gebruik van nieuwe technologieën kan dan ook een belangrijke rol spelen in de evolutie van de

COVID-19. Les applications numériques de traçage de contacts qui sont installées sur un smartphone peuvent aider les soins de santé dans le monitoring et la rupture du nombre de contaminations et la limitation du traçage manuel des contacts. De cette manière, les applications numériques peuvent être un moyen pour les services des soins de santé d'informer la population, de manière plus efficace et moins intrusive pour la vie privée et de les aider dans le suivi d'un éventuel contact avec une personne contaminée. C'est particulièrement important dans le cadre d'une stratégie de sortie dans laquelle les restrictions sur les déplacements sont diminuées et le nombre de contacts entre les individus augmente progressivement.

Les applications numériques de traçage de contacts permettent aux citoyens de constater eux-mêmes qu'ils ont été en contact avec une personne contaminée, sans savoir qui est la personne contaminée et sans que les localisations où ces personnes se sont rendues soient sauvegardées, ni dans l'application de traçage de contacts, ni dans une banque de données centrale. Une exigence fondamentale pour une stratégie de sortie réussie basée sur des technologies numériques est la confiance du citoyen dans ces technologies et la plus grande participation du citoyen à ces technologies. Son utilisation doit donc être encadrée avec les garanties les plus strictes et satisfaire aux exigences en matière des droits fondamentaux. L'application des principes *privacy-by-design* du Règlement général sur la protection des données doit être un élément central dans le développement des applications de traçage de contacts. Le contrôleur européen de la protection des données recommande dans ce domaine les applications numériques de traçage de contacts utilisant Bluetooth et avec un fonctionnement décentralisé, ce qui constitue une méthode qui a également été adoptée dans cette proposition.

L'efficacité d'une application de traçage de contacts est exponentiellement proportionnelle avec le nombre de personnes qui installent et activent cette même application. Le développement des applications de traçage de contacts conformes à la législation en matière de la vie privée et des droits fondamentaux en général n'est donc pas uniquement une exigence de base pour permettre ces technologies, mais c'est aussi une condition fondamentale pour pouvoir garantir l'efficacité de la technologie. Ce n'est que pour autant que le citoyen ait confiance en cette technologie qu'il/elle pourra être convaincu(e) que c'est un moyen nécessaire pour rompre la chaîne des contaminations et qu'il/elle franchira le pas pour y contribuer.

En fin de compte, la décision d'installer et d'utiliser une application de traçage de contacts revient uniquement

COVID-19-pandemie. Digitale contactopsporingsapplicaties die op een smartphone worden geïnstalleerd kunnen de gezondheidsdiensten helpen in het monitoren en doorbreken van het aantal besmettingen en de beperkingen van manuele contactopsporing verhelpen. Zo kunnen deze digitale applicaties een middel zijn voor de gezondheidsdiensten om op meer doeltreffende wijze en op een wijze die de inmenging in de persoonlijke levenssfeer beperkt, de bevolking te informeren en te begeleiden in de opvolging van een mogelijk contact met een besmet persoon. Dit is van bijzonder belang in het kader van een exit-strategie waarbij de beperkingen op verplaatsingen worden teruggeschroefd en het aantal contacten tussen individuen geleidelijk terug toeneemt.

Digitale contactopsporingsapplicaties laten de burgers toe zelf vast te stellen dat ze recent in contact zijn geweest met een besmet persoon, zonder dat ze weten wie de besmette persoon is en zonder dat de plaatsen waar personen geweest zijn, worden bijgehouden, noch in de contactopsporingsapplicatie, noch in een centrale gegevensbank. Een fundamentele vereiste voor een doeltreffende exit-strategie die berust op digitale technologieën is het vertrouwen van de burger in deze technologieën en de grootst mogelijke deelname van de burger aan deze technologieën. Het gebruik ervan moet dan ook met de strengste waarborgen omkaderd zijn en voldoen aan de vereisten inzake de grondrechten. De toepassing van de *privacy-by-design* principes van de Algemene Verordening Gegevensbescherming moet centraal staan bij de ontwikkeling van contactopsporingsapplicaties. Het Europees Comité voor gegevensbescherming beveelt op dit vlak digitale contactopsporingsapplicaties aan die gebruik maken van bluetooth en die gedecentraliseerd werken, een methode waarvoor ook geopteerd wordt in voorliggend voorstel.

De doeltreffendheid van een contactopsporingsapplicatie is exponentieel evenredig met het aantal personen dat eenzelfde applicatie installeert en activeert. Het ontwikkelen van contactopsporingsapplicaties die in overeenstemming zijn met de privacywetgeving en de grondrechten in het algemeen is dus niet alleen een basisvereiste om dergelijke technologie toe te laten, het is een onderliggende voorwaarde om de doeltreffendheid van de technologie te kunnen verzekeren. Het is slechts voor zover de burger vertrouwen heeft in deze technologie dat hij/zij kan overtuigd worden dat dit een noodzakelijk middel is in het doorbreken van de besmettingsketen en de stap zal zetten om hierin zijn/haar bijdrage te leveren.

Ultiem behoort de beslissing om een contactopsporingsapplicatie te installeren en te gebruiken enkel en

au citoyen. Cette proposition opte pour un système où aussi bien l'installation de l'application de traçage de contacts que le téléchargement par une personne contaminée des informations anonymes de contamination dans une liste log centrale se font librement par la personne concernée.

La présente proposition de loi prévoit en outre la possibilité de participer à une recherche épidémiologique. Cette collaboration est entièrement optionnelle (avec une démarche volontaire explicite de l'utilisateur de l'application) et n'est pas essentielle pour le fonctionnement de l'application de traçage de contacts. Dans ce cas, des informations pertinentes sont envoyées tous les jours à une banque de données épidémiologique séparée: il s'agit ici de l'utilisateur de l'application, le statut de l'utilisateur (contaminé ou pas) et des informations sur les contacts avec les personnes contaminées. Aucune information sur la localisation ou le moment précis n'est communiquée. Suite à l'avis 34/2020 de l'Autorité de protection des données (ci-après "APD"), la proposition a été adapté afin de clarifier que la recherche épidémiologique sera effectuée sur base de données anonymisées, en non pas des données pseudonymisées tel qu'il était indiqué dans la proposition auparavant. L'identité de chaque utilisateur est remplacée par une clé aléatoire (la clé sécurisée). Cette clé ne permet pas de retourner au nom de l'utilisateur puisqu'elle a été choisie de façon aléatoire, sans aucun lien avec des données à caractère personnel. Techniquement, on parle d'un pseudonyme mais juridiquement il s'agit bien d'une donnée anonyme.

Une utilisation large, par les citoyens, des applications de traçage de contacts développées selon le principe du *privacy-by-design* permet d'effectuer ce traçage de contacts d'une manière beaucoup moins intrusive dans la vie privée des citoyens que d'autres méthodes de traçage de contacts. Stimuler l'utilisation large par les citoyens d'une seule application de traçage de contacts, développée selon le principe du *privacy-by-design* est donc une mesure qui est parfaitement conforme au principe prévu dans le Règlement général sur la protection des données qui stipule qu'on doit choisir des mesures qui permettent d'atteindre les objectifs prévus de la manière la plus efficace et la moins intrusive sur le plan du droit à la protection de la vie privée.

Vu le caractère entièrement volontaire de l'utilisation des applications de traçage de contacts, et le fait que l'utilisation du système DP^{3}T minimalise l'intrusion dans la vie privée, l'utilisation de ces applications établit un juste équilibre entre le droit à la santé d'une part et l'intrusion à la vie privée d'autre part.

alleen toe aan de burger. Dit voorstel opteert voor een systeem waarbij zowel de installatie van de contactopsporingsapplicatie als het opladen door een besmet persoon van de anonieme contactinformatie in een centrale loglijst gebeurt vrijwillig door de betrokkene.

Daarnaast voorziet dit voorstel in de mogelijkheid om mee te werken aan epidemiologisch onderzoek. Deze medewerking is volledig optioneel (met expliciete opt-in van de app-gebruiker) en is niet essentieel voor de werking van de contactopsporingsapplicatie. In dit geval wordt op dagelijkse basis relevante informatie naar een afzonderlijke epidemiologische database verzonden: het gaat hier om de gebruiker van de applicatie, de status van die gebruiker (besmet of niet) en informatie over de contacten met besmette personen. Er wordt geen informatie over locatie of het precieze tijdstip meegedeeld. Ingevolge het advies 34/2020 van de Gegevensbeschermingsautoriteit (hierna "GBA") werd het voorstel aangepast om te verduidelijken dat het epidemiologisch onderzoek op basis van geanonimiseerde gegevens zal gebeuren, en niet gepseudonimiseerde gegevens zoals eerder in het voorstel stond. De identiteit van elke gebruiker wordt vervangen door een random sleutel (de beveiligde sleutel). Het is niet mogelijk om vanuit die sleutel terug te keren naar de naam van de gebruiker want de sleutel is willekeurig gekozen, totaal onafhankelijk van enig persoonsgegeven. Technisch wordt hierbij gesproken over een pseudoniem maar juridisch gaat het wel degelijk over een anoniem gegeven.

Een ruim gebruik, door de burgers, van contactopsporingsapplicaties die zijn ontwikkeld volgens het principe van *privacy by design*, laat toe om contactopsporing te verrichten op een wijze die veel minder invasief is in de persoonlijke levenssfeer van de burgers dan andere methoden van contactopsporing. Het stimuleren van een ruim gebruik door de burgers van eenzelfde contactopsporingsapplicatie, ontwikkeld volgens het principe van *privacy by design*, is dus een maatregel die volledig strookt met het principe vastgelegd in de Algemene Verordening Gegevensbescherming dat stelt dat moet worden gekozen voor maatregelen die toelaten vooropgestelde doeleinden te bereiken op de meest effectieve wijze en op een manier die het minst invasief is op het vlak van de het recht op bescherming van de persoonlijke levenssfeer.

Gelet op het volledig vrijwillig karakter van het gebruik van de contactopsporingsapplicaties, en het feit dat het gebruik van het DP^{3}T systeem de inmenging op het vlak van het privéleven minimaliseert, vindt het gebruik van dergelijke applicaties de juiste balans tussen het recht op gezondheid enerzijds en de inmenging op het vlak van het privéleven anderzijds.

La présente proposition de loi a pour objectif de garantir l'utilisation d'une seule méthode technologique d'applications de traçage de contacts sur le territoire belge, qui minimalise le traitement des données à caractère personnel et qui est basée au maximum sur un code open source public qui peut être vérifié par des experts indépendants. Cette méthode technologique est le système DP³T. Dans ce sens, cette proposition répond donc à la recommandation de l'APD dans son avis 34/2020 consistant à demander de publier le code-source. La description et le code-source du système DP³T est en effet complètement public. Toutes les applications de traçage de contacts utilisées en Belgique doivent être basées sur le système DP³T, conformément à la présente loi. Cela devrait permettre de maximiser l'efficacité et minimiser l'intrusion dans la vie privée. Toutefois, rien n'empêche que différents fournisseurs d'applications de traçage de contacts proposent différentes interfaces d'utilisateurs.

Le traçage des contaminations COVID-19, et donc aussi le développement des applications numériques de traçage de contacts, relèvent de la compétence des entités fédérées. Néanmoins, le niveau fédéral est compétent pour la création d'un cadre juridique relatif aux garanties en matière de la protection des données à caractère personnel auxquelles ces applications de traçage de contacts doivent satisfaire. Les fonctionnalités, les modalités et les exigences techniques pour l'utilisation d'applications numériques de traçage de contacts prévues dans le présent arrêté se limitent à ce qui est strictement nécessaire pour pouvoir déterminer ces garanties en matière de protection des droits et libertés fondamentaux des citoyens, et en particulier la protection des informations traitées.

La présente loi porte uniquement sur les applications de traçage de contacts. D'autres applications e-Health, comme les applications de triage, d'auto-monitoring, de monitoring dans le cadre d'une relation de soins ou des applications pour les soins à distance ne sont pas régies par la présente loi. Lorsque ces applications traitent des données à caractère personnel, le Règlement général sur la protection des données est pleinement d'application. L'APD a formulé des recommandations précieuses auxquelles ces applications doivent remplir pour être conformes au Règlement général sur la protection des données. Le système de formulation des recommandations aux personnes contaminées ou aux contacts de ces personnes contaminées est donc exclu du champ d'application de la présente loi et se fera conformément à la réglementation en vigueur.

Dit wetsvoorstel heeft tot doel om ervoor te zorgen dat op het Belgisch grondgebied slechts één technologische methode van contactopsporingsapplicaties wordt gebruikt die de verwerking van persoonsgegevens minimaliseert en maximaal gebaseerd is op openbare open source code die door onafhankelijke experten kan worden geverifieerd. Deze technologische methode is het DP³T systeem. In die zin komt dit voorstel dus tegemoet aan de aanbeveling van de GBA in haar advies 34/2020 om de broncode te publiceren. De beschrijving en de broncode van het DP³T systeem is immers volledig openbaar. Alle contactopsporingsapplicaties die in België worden gebruikt, dienen overeenkomstig deze wet gebaseerd te zijn op het DP³T systeem. Dit moet ervoor zorgen dat de doeltreffendheid wordt gemaximaliseerd en de inmenging op het vlak van het privéleven wordt geminimaliseerd. Niets belet echter dat door verschillende aanbieders van contactopsporingsapplicaties verschillende gebruikersinterfaces worden aangeboden.

Het opsporen van COVID-19-besmettingen, en dus ook de ontwikkeling van digitale contactopsporingsapplicaties, behoort tot de bevoegdheid van de deelstaten. Het federaal niveau is echter bevoegd voor het creëren van het algemeen juridisch kader voor wat betreft de nodige waarborgen op het niveau van de bescherming van persoonsgegevens waaraan deze contactopsporingsapplicaties moeten voldoen. De functionaliteiten, de modaliteiten en de technische voorwaarden voor het gebruik van digitale contactopsporingsapplicaties die in dit besluit worden bepaald beperken zich tot wat strikt noodzakelijk is om de waarborgen ter bescherming van de fundamentele rechten en vrijheden van de burgers, en in het bijzonder de bescherming van de verwerkte informatie, te kunnen bepalen.

Deze wet handelt enkel over contactopsporingsapplicaties. Andere e-Gezondheidsapplicaties, zoals applicaties voor triage, zelfmonitoring, monitoring in het kader van een zorgrelatie of applicaties voor zorg op afstand, worden niet door deze wet geregeld. Wanneer door dergelijke applicaties persoonsgegevens worden verwerkt, is hierop de Algemene Verordening Gegevensbescherming onverkort van toepassing. De GBA heeft waardevolle aanbevelingen geformuleerd waaraan deze applicaties dienen te voldoen om in overeenstemming te zijn met de Algemene Verordening Gegevensbescherming. Het systeem voor het formuleren van aanbevelingen aan besmette personen of contacten van besmette personen valt dus buiten het toepassingsgebied van deze wet en zal geschieden overeenkomstig de geldende regelgeving.

2. *L'utilisation d'une application numérique de traçage de contacts et la confirmation d'une contamination COVID-19*

Le fonctionnement du processus est décrit ci-dessous, cependant, seul le fonctionnement de l'application elle-même est prévue dans cette proposition.

Une personne ayant installé une application de traçage de contacts sur son smartphone pense qu'il/elle est contaminé(e) avec le COVID-19 et se dirige vers un prestataire de soins. Si le prestataire de soins confirme que cette présomption est correcte, un échantillon est prélevé et envoyé au laboratoire de référence. Le prestataire de soins donne une prescription pour le test avec le numéro NISS de l'utilisateur de l'application, le numéro de téléphone du patient et la date de la demande du test COVID-19. Le numéro de téléphone du patient est nécessaire pour pouvoir contacter le patient pour le traçage des contacts en cas de contamination.

Si l'utilisateur a installé l'application numérique de traçage de contacts, il communique à son tour via l'application son numéro de téléphone et la date du test à Sciensano via l'application. En parallèle, l'application envoie également des informations (anonymisées) qui permettent à l'application numérique de traçage de contacts de vérifier l'authenticité (mais pas donc pas l'identité) et l'intégrité des données dans l'application.

À part le numéro de téléphone et la date du test, toutes les informations envoyées sont du "charabia" qui ne contient aucune information sur l'identité de la personne. Ce charabia est nécessaire afin d'éviter que quelqu'un d'autre puisse s'enregistrer faussement comme étant contaminé.

L'application de traçage de contacts envoie un code de vérification pour confirmer le test avec le prestataire des soins. Les deux parties – le prestataire de soins et l'utilisateur de l'application – vérifient la correspondance de ces tests et confirment alors le test.

Lorsque le résultat du test est connu et positif, l'utilisateur de l'application est contacté par un prestataire de soins de santé. Celui-ci détermine – avec l'utilisateur de l'application la date à laquelle le patient est présumé avoir été contaminé. Il est demandé à l'utilisateur de l'application d'indiquer dans l'application qu'il/elle est contaminé(e). À ce moment, l'utilisateur peut encore décider de le faire ou non.

Dès que l'utilisateur indique dans l'application de traçage de contacts qu'il est contaminé par le COVID-19, Sciensano vérifie l'authenticité de l'application de traçage de contacts et envoie un sms de vérification à l'utilisateur

2. *Het gebruik van een digitale contactopsporingsapplicatie en de bevestiging van een COVID-19-besmetting*

De werking van het proces wordt hieronder beschreven, echter, enkel de werking van de applicatie zelf wordt door voorliggend voorstel geregeld.

Een persoon die een contactopsporingsapplicatie op zijn/haar smartphone heeft geïnstalleerd vermoedt dat hij/zij besmet is met COVID-19 en gaat naar een zorgverlener. Als de zorgverlener bevestigt dat dit vermoeden correct is, wordt een staal afgenomen en naar een referentielabo gestuurd. De zorgverlener schrijft een voorschrift voor de test met het INSZ nummer van de patiënt, het telefoonnummer van de patiënt en de datum van de aanvraag van de COVID-19 test. Het telefoonnummer van de patiënt is nodig om de patiënt in geval van besmetting te kunnen contacteren voor contactopsporing.

Indien de gebruiker een contactopsporingsapplicatie heeft geïnstalleerd, geeft de gebruiker op zijn/haar beurt via zijn applicatie aan Sciensano zijn/haar telefoonnummer en datum van de test door. De applicatie stuurt tegelijk ook (geanonimiseerde) informatie mee die de contactopsporingsapplicatie moet toelaten de authenticiteit (maar dus geenszins de identiteit) en de integriteit van de gegevens in de applicatie te verifiëren.

Op het telefoonnummer en de datum van de test na, is alle verstuurde informatie "wartaal" die geen informatie over de identiteit van de persoon bevat. Deze wartaal is nodig om te vermijden dat iemand anders zich valselijk als besmet kan registreren.

De contactopsporingsapplicatie stuurt een verificatiecode op om de test met de zorgverlener te bevestigen. Beide partijen – de zorgverlener en de app-gebruiker – verifiëren dat deze codes overeenkomen en bevestigen dan de test.

Wanneer het resultaat van de test gekend is en positief, wordt de app-gebruiker gecontacteerd door een zorgverlener. Deze bepaalt samen met de app-gebruiker bepaald op welke datum de patiënt vermoedelijk besmettelijk is geworden. De app-gebruiker wordt gevraagd om in de applicatie aan te geven dat hij/zij besmet is. De gebruiker kan op dit moment nog beslissen om dit niet te doen.

Zodra de gebruiker in de contactopsporingsapplicatie aangeeft dat hij/zij met COVID-19 is besmet, verifieert Sciensano de authenticiteit van de contactopsporingsapplicatie en stuurt het een sms naar de app-gebruiker

de l'application. Après l'introduction du code sms dans l'application, Sciensano donne l'autorisation à l'application (sous la forme d'un message numérique signé) de télécharger la clé sécurisée et la date de la contamination présumée vers une liste log centrale contenant les clés sécurisées de tous les patients contaminés par le COVID-19.

La clé sécurisée de l'utilisateur de l'application chez qui la contamination par le COVID-19 a été confirmée et transférée via l'application est téléchargée avec l'autorisation. Après validation de l'autorisation et de l'intégrité de la clé sécurisée, la clé sécurisée est rendue disponible via une liste log centrale pour les applications de traçage de contacts d'autres utilisateurs.

3. ***Le fonctionnement du traçage de contacts***

Le smartphone d'un utilisateur d'une application numérique de traçage de contacts génère une ou plusieurs clés sécurisées uniques. Sur base de ces clés sécurisées, le smartphone établit des numéros de séries aléatoires à intervalles réguliers.

Le smartphone de l'utilisateur envoie ensuite à intervalles réguliers un numéro de série à tous les smartphones à proximité. Les numéros de série ne contiennent pas d'informations sur l'identité ou la localisation de l'utilisateur de l'application. Pendant que le smartphone envoie les numéros de séries, il "écoute" également les numéros de série des autres smartphones à proximité sur lesquels est également installée une application interopérable. Si les smartphones restent pendant un certain temps (quelques secondes) à proximité, ils échangent de numéro de série; ils stockent des numéros de série correspondant à des rencontres qui durent plus de 30 secondes et ayant une certaine force du signal minimum. Les deux smartphones sauvegardent tous les numéros de série qu'ils ont entendu pendant maximum trois semaines.

Lorsqu'il est constaté que l' utilisateur de l'application est contaminé par le COVID-19, et que cet utilisateur l'indique volontairement dans l'application, sa clé sécurisée d est rendue disponible pour les autres utilisateurs de l'application. Des précautions techniques nécessaires ont été prises pour pouvoir garantir qu'une constatation de contamination avec le COVID-19 est réellement liée à 1) l'utilisateur de l'application chez qui la contamination a été constatée et 2) le smartphone de l'utilisateur de l'application.

La liste log centrale sauvegarde les clés sécurisée des utilisateurs de l'application qui ont confirmé une contamination par le COVID-19 via leur application. La liste log centrale ne reçoit pas d'informations sur la

ter verificatie. De app-gebruiker toetst vervolgens een sms-code in de applicatie waarop Sciensano vervolgens een autorisatie aan de applicatie (in de vorm van een digitaal ondertekend bericht) geeft om de beveiligde sleutel en de datum van vermoedelijke besmetting op te laden naar een centrale loglijst met de beveiligde sleutels van alle met COVID-19 besmette patiënten.

De beveiligde sleutel van de app-gebruiker bij wie een COVID-19-besmetting werd vastgesteld en doorgegeven via de applicatie wordt samen met de autorisatie opgeladen. Na validatie van de autorisatie en de integriteit van de beveiligde sleutel wordt de beveiligde sleutel door een centrale loglijst beschikbaar gemaakt voor de contactopsporingsapplicaties van andere gebruikers.

3. ***De werking van de contactopsporing***

De smartphone van een gebruiker van een digitale contactopsporingsapplicatie genereert een of meerdere unieke beveiligde sleutels. Op basis van deze beveiligde sleutels maakt de smartphone willekeurige serienummers op geregelde tijdstippen.

De smartphone van de app-gebruiker stuurt vervolgens op geregelde tijdstippen een serienummer naar alle smartphones in de buurt. De serienummers bevatten geen informatie over de identiteit of de locatie van de app-gebruiker. Terwijl de smartphone de serienummers stuurt "luistert" deze ook naar de serienummers van andere smartphones in de buurt, waarop eveneens een interoperabele applicatie is geïnstalleerd. Als de smartphones langer dan een bepaalde tijd (een paar seconden) in elkaars buurt blijven wisselen ze serienummers uit; ze bewaren serienummers overeenkomend met ontmoetingen die langer dan 30 seconden duren en een minimum signaalsterkte hebben. Beide smartphones bewaren alle serienummers die ze hebben gehoord gedurende maximaal drie weken.

Wanneer bij een app-gebruiker een COVID-19-besmetting wordt vastgesteld, en de app-gebruiker dit op vrijwillige basis aangeeft in de app, dan wordt de beveiligde sleutel van de app-gebruiker via een centrale loglijst beschikbaar gemaakt voor andere gebruikers van de applicatie. Technisch worden de nodige voorzorgen genomen om te kunnen garanderen dat de vaststelling van een COVID-19-besmetting daadwerkelijk gelinkt wordt aan 1) de app-gebruiker bij wie de besmetting wordt vastgesteld en 2) de smartphone van de app-gebruiker.

De centrale loglijst slaat de beveiligde sleutels op van de app-gebruikers die via hun applicatie een COVID-19-besmetting hebben bevestigd. De centrale loglijst krijgt geen informatie over de locatie van de app-gebruiker, in

localisation de l'utilisateur de l'application, à proximité de qui il/elle a été ou même combien de personnes il/elle a vu. La proposition prévoit également que dès que la clé sécurisée ou les clés sécurisées arrivent dans la liste log, elles ne peuvent plus être utilisées par l'équipement terminal de l'utilisateur et sont retirées de l'équipement terminal de l'utilisateur. Les données qui sont sauvegardées dans la liste log même ne peuvent pas être conservées plus longtemps que trois semaines après leurs intégration dans la liste log. Selon les directives protection des données de la Commission européenne les données peuvent être conservées pendant maximum un mois (période d'incubation + une certaine marge). Il est estimé dans cette proposition qu'un délai de trois semaines doit suffire et est nécessaire afin de réaliser les objectifs visés. En effet, vu l'incertitude dans le monde médical sur la durée exacte de la période de contamination (pour COVID-19 il ne s'agit pas de la période d'incubation puisque certains patients n'ont pas de symptômes) un délai de trois semaines est opportun.

Les smartphones d'autres utilisateurs qui ont installé l'application de traçage de contacts établissent régulièrement des contacts avec la liste log centrale.Le téléphone vérifie s'il a entendu des numéros de série basés sur ces clés sécurisées provenant de téléphones qui se trouvaient à proximité au cours des derniers jours. Si le smartphone a entendu un nombre de numéros de série COVID-19 avec une certaine force minimale les derniers trois semaines, il avertit le téléphone de l'utilisateur.

Le gouvernement détermine quel sera le message qui sera communiqué via le smartphone à l'utilisateur de l'application. Il peut par exemple s'agir d'un message qu'il est possible que l'utilisateur de l'application ait été en contact avec une personne contaminée par le COVID-19.

L'utilisateur peut choisir d'éteindre l'application temporairement (par exemple pendant une période où il est seul à la maison). Pendant cette période, aucun numéro de série ne sera envoyé ou entendu.

Il est prévu une interopérabilité et donc une efficacité de l'application de traçage de contacts aussi large que possible. Il faut pouvoir échanger les informations de la liste log centrale avec d'autres pays.

wiens nabijheid hij/zij was of zelfs hoe veel mensen hij/zij heeft gezien. Het voorstel bepaalt ook dat de beveiligde sleutel of sleutels, eens zij terechtkomen in de loglijst, niet meer mogen gebruikt worden door de eindapparatuur van de gebruiker en dus worden verwijderd uit de eindapparatuur van de gebruiker. De gegevens die in de loglijst zelf worden opgeslagen mogen niet langer bewaard worden dan drie weken nadat ze in de loglijst werden opgenomen. Volgens de privacyrichtlijnen van de Europese Commissie mogen de gegevens maximaal een maand bewaard worden (incubatieperiode + een zekere marge). In dit voorstel wordt een termijn van drie weken voldoende en noodzakelijk geacht om de doelstellingen te bereiken. Inderdaad, gelet op de onzekerheid die nog heerst in de medische wereld over de exacte duurtijd van de besmettelijke periode (bij COVID-19 is dit niet de incubatietijd omdat sommige patiënten geen symptomen vertonen) is een termijn van drie weken opportuun.

De smartphones van andere gebruikers die de contactopsporingsapplicatie geïnstalleerd hebben maken op geregelde tijdstippen contact met de centrale loglijst. De smartphone verifieert of het serienummers gebaseerd op deze beveiligde sleutels heeft gehoord van smartphones die nabij waren in de afgelopen drie weken. De telefoon kijkt of hij serienummers gebaseerd op deze beveiligde sleutels heeft gehoord van telefoons die nabij waren in de afgelopen dagen. Als de telefoon gedurende de afgelopen de 3 weken aantal COVID-19-serienummers heeft gehoord met een bepaalde minimum sterkte, dan waarschuwt de telefoon de gebruiker.

De overheid bepaalt het bericht dat in dat geval door de smartphone aan de app-gebruiker wordt meegedeeld. Het kan bijvoorbeeld gaan om een bericht dat de app-gebruiker mogelijks in contact is geweest met een persoon bij wie een COVID-19-besmetting werd vastgesteld.

De gebruiker kan er voor kiezen om de applicatie tijdelijk uit te schakelen (bijvoorbeeld tijdens een periode dat hij/zij alleen thuis is). Er worden tijdens deze periode dan geen serienummers verstuurd of gehoord.

Er wordt voorzien in een zo ruim mogelijke interoperabiliteit en dus doeltreffendheid van de contactopsporingsapplicatie. Informatie uit de centrale loglijst moet kunnen worden uitgewisseld met informatie uit loglijsten van andere landen.

4. ***Garanties en vue de préserver les droit fondamentaux et en particulier la protection des données à caractère personnel***

La présente loi détermine le cadre juridique dans lequel les applications de traçage de contacts doivent fonctionner. Lors de l'établissement cette loi, il a été tenu compte des recommandations des instances compétentes nationales et internationales, en particulier la Commission européenne, le Comité européen de la protection des données et l'Autorité belge de protection des données.

En première instance, le test de nécessité et de proportionnalité a déjà été exposé en détail sous le rubrique 1. Ensuite, comme confirmé par les instances susvisées, la législation européenne sur la vie privée prévoit une base légale pour le développement et l'utilisation des applications de traçage de contacts, en particulier les articles 6, § 1er, e) et 9, § 2, i) du Règlement général sur la protection des données. La présente loi se prévaut donc de ces bases juridiques spécifiques.

La présente loi prévoit une base légale afin d'atteindre trois objectifs:

— en premier lieu une application numérique de traçage de contacts doit pouvoir confirmer une contamination par le COVID-19 d'un utilisateur de l'application;

— la confirmation de la contamination doit ensuite permettre de pouvoir dépister les contacts de l'utilisateur de l'application contaminé par le COVID-19 pour qu'ils puissent être avertis qu'ils ont été à proximité d'une personne contaminée;

— finalement, on a créé un cadre pour pouvoir utiliser, sur base des données anonymisées, certains traitements fait par les applications de traçage de contacts à des fins de recherche épidémiologique. Il s'agit par exemple de recherches du degré de contact de l'épidémie COVID-19.

Ce cadre légal est nécessaire, mais on ne peut pas le confondre avec le libre choix du citoyen d'installer, d'utiliser et de désinstaller une application de traçage de contacts. La présente loi détermine le cadre pour les garanties techniques et en matière des droits de l'homme auxquelles les applications doivent satisfaire, mais n'impose en aucun cas une obligation au citoyen d'installer, d'utiliser ou de désinstaller l'application de traçage de contacts. Par exemple, un employeur ne peut en aucun cas imposer l'installation et l'utilisation d'une application de traçage de contacts. Sur recommandation de l'APD dans son avis 34/2020 il est également précisé qu'un (non-)utilisateur ne peut aucunement subir un désavantage ou un avantage sur base d'une (non-)

4. ***Waarborgen ter vrijwaring van de grondrechten en in het bijzonder de bescherming van persoonsgegevens***

Deze wet bepaalt het juridisch kader waarbinnen de contactopsporingsapplicaties mogen functioneren. Bij het opstellen van deze wet werd rekening gehouden met de aanbevelingen van de bevoegde nationale en internationale instanties, in het bijzonder de Europese Commissie, het Europees Comité voor Gegevensbescherming en de Belgische Gegevensbeschermingsautoriteit.

In de eerste plaats werd onder punt 1 reeds uitvoerig de noodzakelijkheids- en evenredigheidstoets toegelicht. Vervolgens, zoals bevestigd door hogergenoemde instanties, voorziet de Europese privacywetgeving in een wettelijke basis voor de ontwikkeling en het gebruik van contactopsporingsapplicaties, in het bijzonder artikelen 6, § 1, e) en 9, § 2, i) van de Algemene Verordening Gegevensbescherming. Deze wet beroept zich dan ook op deze specifieke wettelijke grondslagen.

Deze wet voorziet in de wettelijke grondslag om drie doelstellingen te verwezenlijken:

— in de eerste plaats dient een digitale contactopsporingsapplicatie een COVID-19-besmetting van een app-gebruiker te kunnen bevestigen;

— de bevestiging van de besmetting moet vervolgens toelaten om de contacten van de met COVID-19 besmette app-gebruiker te kunnen opsporen zodat zij verwittigd kunnen worden dat zij zich in de nabijheid van deze besmette persoon hebben bevonden;

— tot slot wordt ook een kader gecreëerd om op basis van geanonimiseerde gegevens bepaalde van de verwerkingen door de contactopsporingsapplicaties te kunnen gebruiken voor epidemiologisch onderzoek. Het betreft bijvoorbeeld het onderzoeken van de contactgraad van de COVID-19 epidemie.

Dit wettelijk kader is noodzakelijk maar mag niet verward worden met de vrije keuze van de burger om een contactopsporingsapplicatie te installeren, te gebruiken en te de-installeren. Deze wet bepaalt het kader voor de technische en mensenrechtelijke waarborgen waaraan de applicaties dienen te voldoen maar legt op geen enkele wijze een verplichting op aan de burger om de contactopsporingsapplicatie te installeren, te gebruiken of te de-installeren. Zo mag bijvoorbeeld een werkgever in geen geval aan zijn werknemers het installeren en gebruiken van een contactopsporingsapplicatie opleggen. Op aanbeveling van de GBA in haar advies 34/2020 wordt ook verduidelijkt dat een (niet-) gebruiker op geen enkele manier een nadeel of een

utilisation d'une application de traçage de contacts. En revanche, la suggestion de l'APD de prévoir des sanctions civiles et/ou administratives et/ou pénales pour les personnes qui lieraient l'accès à un bien ou à un service à l'utilisation de cette application n'est pas suivie. Comme déjà exposé, l'efficacité d'une application de traçage de contacts est exponentiellement proportionnelle avec le nombre de personnes qui l'installent et l'utilisent. Des campagnes de promotion pour l'utilisation d'une application seront donc envisagées. Afin de ne pas freiner l'encouragement du citoyen à installer une application cette proposition n'impose pas des sanctions autres que de référer indirectement aux sanctions déjà applicables en vertu de législation en vigueur telle que par exemple la législation en matière de non-discrimination. En plus, le caractère libre de l'installation d'une application est mis en avant à plusieurs reprises dans cette proposition.

L'installation d'une application de traçage de contacts active un certain nombre d'actions comme décrites au point 3, notamment la génération de clés sécurisées et de numéros de série temporaires aléatoires. Cela se fait de manière anonymisée. Ensuite il revient *in fine* à l'utilisateur d'une application de traçage de contacts d'actionner activement et volontairement via l'application les autres mécanismes techniques sus mentionnés par le biais de la confirmation d'une contamination par le COVID-19. Il va sans dire que c'est une étape nécessaire dans la réalisation de l'objectif ultime d'une application de traçage de contacts, à savoir limiter l'épidémie COVID-19.

La confiance et la collaboration du citoyen sont donc primordiaux. Vu les inquiétudes sur l'éventuel impact considérable de ces applications de traçage de contacts sur l'exercice de nos droits de base et sur les valeurs de notre société démocratique, la présente loi prévoit des garanties strictes pour préserver les droits fondamentaux et en particulier la protection des données à caractère personnel. Le traitement des données à caractère personnel par ces applications de traçage de contacts est limité à un stricte minimum, conformément à la législation européenne et nationale en la matière, afin de pouvoir réaliser les objectifs prévus.

Une application de traçage de contacts sur base du système DP^{3}T sauvegarde uniquement des données entièrement anonymes sur l'équipement final de l'utilisateur, sans référence à l'identité des personnes qui sont entrées en contact les unes avec les autres, ni la localisation où le contact a eu lieu. Le moment approximatif auquel le contact a eu lieu est sauvegardé, parce qu'il est nécessaire pour pouvoir constater si le contact

voordeel mag ondervinden op grond van het al dan niet gebruiken van een contactopsporingsapplicatie. De suggestie van de GBA daarentegen, om te voorzien in burgerlijke/administratieve/strafrechtelijke sancties voor degenen die de toegang tot een goed of dienst zouden koppelen aan het gebruik van deze applicatie, wordt niet gevolgd. Zoals reeds eerder uiteengezet is de doeltreffendheid van een contactopsporingsapplicatie exponentieel evenredig met het aantal personen dat eenzelfde applicatie installeert en gebruikt. Promotiecampagnes voor het gebruik van een applicatie zullen dus voorzien worden. Teneinde aanmoedigingen van de burger om een applicatie te installeren niet te remmen legt dit voorstel geen sancties op anders dan indirect te verwijzen naar reeds toepasselijke sancties krachtens bestaande wetgeving zoals bijvoorbeeld de wetgeving inzake nondiscriminatie. Bovendien wordt het vrijwillig karakter van het installeren van een applicatie herhaaldelijk naar voren geschoven in dit voorstel.

Het installeren van een contactopsporingsapplicatie activeert een aantal technische handelingen zoals omschreven in punt 3, met name het genereren van beveiligde sleutels en tijdelijk willekeurige serienummers. Dit gebeurt op geanonimiseerde wijze. Vervolgens komt het nog altijd aan de gebruiker van een contactopsporingsapplicatie toe om al dan niet actief en op vrijwillige basis de overige technische handelingen te activeren aan de hand van het bevestigen van een COVID-19-besmetting via de applicatie. Het spreekt voor zich dat dit een noodzakelijke stap is om de ultieme doelstelling van een contactopsporingsapplicatie, het terugdringen van de COVID-19-epidemie, te helpen verwezenlijken.

Het vertrouwen en de medewerking van de burger is bijgevolg cruciaal. Gelet op de bezorgdheden die bestaan omtrent de mogelijks verregaande impact van dergelijke contactopsporingsapplicaties op de uitoefening van onze basisrechten en op de waarden van onze democratische samenleving voorziet deze wet dan ook in strikte waarborgen ter vrijwaring van de grondrechten en in het bijzonder van de bescherming van de persoonsgegevens. De verwerking van persoonsgegevens door deze contactopsporingsapplicaties wordt, overeenkomstig de Europese en nationale wetgeving ter zake, beperkt tot het strikte minimum om de vooropgestelde doelstellingen te verwezenlijken.

Een contactopsporingsapplicatie op basis van het DP^{3}T systeem slaat enkel volledig anonieme gegevens op de eindapparatuur van de gebruiker op, zonder verwijzing naar de identiteit van de personen waartussen het contact heeft plaatsgevonden, noch naar de plaats waar het contact heeft plaatsgevonden. Het benaderend tijdstip waarop het contact heeft plaatsgevonden wordt wel bewaard omdat dit nodig is om te kunnen vaststellen

a eu lieu entre le début de la contagiosité et la constatation de la contamination. Les données générées dans l'équipement final de l'utilisateur ne sont d'ailleurs pas communiquées à d'autres utilisateurs.

L'utilisation du numéro de téléphone est nécessaire pour pouvoir constater avec certitude que la personne qui indique qu'il/elle est contaminé(e) l'est réellement. Si on peut faire des fausses déclarations concernant la contamination, on demandera erronément aux contacts de prendre des mesures. Il est à ce titre inacceptable par exemple qu'un étudiant qui est entré en contact avec d'autres étudiants les derniers jours puisse mentionner une fausse contamination, ce qui impliquera que tous les autres étudiants avec qui il a été en contact devront s'auto-isoler indûment ou prendre d'autres mesures.

Une garantie supplémentaire est l'impossibilité de croiser des données sauvegardées. Il est primordial que les données des différents banques de données chez Sciensano ne soient pas liées à d'autres banques de données, en particulier avec des banques de données qui contiennent le numéro de téléphone de la personne concernée. Le responsable de traitement doit strictement respecter cela, aussi par rapport à d'autres banques de données qu'il gère lui-même. Vu l'expertise pointue de Sciensano en matière de protection des données relatives à la santé à des fins de recherche scientifique et l'implémentation de méthodes solides en matière de sécurisation et de pseudonymisation des données, Sciensano semble le responsable le plus apte pour ce traitement.

Finalement, il est aussi explicitement prévu que la non installation, la non utilisation et la non désinstallation d'une application de traçage de contacts ne peut donner en aucun cas lieu à une mesure quelconque civile ou pénale, ni à quelconque action discriminatoire.

La présente loi répond à tous les principes de la législation relative à la protection des données:

• elle détermine les finalités pour lesquelles les applications de traçage de contacts peuvent traiter les données;

• elle désigne le responsable du traitement qui doit appliquer les garanties prévues par la présente loi dans le stricte cadre des objectifs décrits. Sciensano est la meilleure institution à cet effet. L'Art. 4, § 1 de la loi du 25 février 2018 portant création de Sciensano détermine que cette institution accomplit certaines tâches en matière de santé, aussi bien au niveau fédéral, régional

of het contact heeft plaatsgevonden tussen het begin van de besmettelijkheid en de vaststelling van de besmetting. De op de eindapparatuur van een gebruiker gegenereerde gegevens worden bovendien niet aan andere gebruikers meegedeeld.

Het gebruik van het telefoonnummer is vereist om met absolute zekerheid te kunnen vaststellen dat de persoon die meldt dat hij/zij besmet is, dat ook effectief is. Indien een valse melding kan geschieden, worden immers diens contacten onterecht gevraagd maatregelen te nemen. Het is bijvoorbeeld niet aanvaardbaar dat een student, die de voorbije dagen in contact geweest is met medestudenten, een valse melding van besmetting zou kunnen uitsturen waardoor alle andere medestudenten waarmee hij in contact is geweest, ten onrechte in zelfisolatie moeten gaan of andere maatregelen zouden moeten treffen.

Een bijkomende waarborg is de onmogelijkheid om de bewaarde gegevens te kruisen. Het is van cruciaal belang dat de gegevens uit de verschillende gegevensbanken bij Sciensano niet worden gekoppeld met andere gegevensbanken, in het bijzonder met gegevensbanken die het telefoonnummer van de betrokken persoon bevatten. De verwerkingsverantwoordelijke dient daarop strikt toe te zien, ook t.o.v. andere gegevensbanken die zij zelf beheert. Gelet op de bijzondere ervaring bij Sciensano inzake de gegevensbescherming bij de omgang met gezondheidsgegevens voor wetenschappelijk onderzoek en het implementeren van degelijke methoden van beveiliging en pseudonimisering van gegevens, lijkt Sciensano de meest aangewezen verantwoordelijke voor deze verwerking te zijn.

Tot slot wordt ook uitdrukkelijk voorzien dat het niet installeren, het niet gebruiken en het niet de-installeren van een contactopsporingsapplicatie op geen enkele wijze aanleiding mag geven tot enige burgerrechtelijke of strafrechtelijke maatregel noch tot enige discriminerende handeling.

Deze wet beantwoordt aan alle principes van het gegevensbeschermingsrecht:

• het bepaalt de doeleinden waarvoor de contactopsporingsapplicaties gegevens mogen verwerken;

• het duidt de verwerkingsverantwoordelijke aan die de waarborgen voorzien door deze wet moet toepassen binnen het strikte kader van de omschreven doelstellingen. Sciensano is daarvoor de best geplaatste instelling. Art. 4, § 1 van de wet van 25 februari 2018 tot oprichting van Sciensano bepaalt dat deze instelling zowel op het federale, gewestelijke en gemeenschapsniveau, alsmede

et communautaire, qu'européen et international, en particulier des recherches scientifiques et des évaluations de risques;

• elle détermine les catégories de données, aussi bien les données à caractère personnel que les données non identifiables (informations) qui peuvent être traitées par l'application de traçage de contacts;

• elle souligne la possibilité pour un utilisateur d'une application de traçage de contacts de garder le contrôle sur ses données et d'avoir le choix d'effacer entièrement ou partiellement ses données;

• elle souligne la transparence en matière d'informations à communiquer à l'utilisateur d'une application de traçage de contacts;

• elle détermine le délai de conservation valable pour les données collectées;

• elle garantit que les données sont collectées soit dans une liste log soit dans une banque de données séparée selon l'objectif du traitement;

• elle interdit le traitement des données collectées à d'autres fins;

• elle impose des exigences techniques et organisationnelles pour le responsable du traitement afin de garantir que les données collectées soient protégées contre le traitement illicite ou illégal et contre les pertes accidentelles, la destruction ou la détérioration;

• elle prévoit que les applications de traçage de contacts soient auto-extinguibles afin de garantir qu'aucune donnée ne soit plus sauvegardée à partir du moment où la fin de l'état d'épidémie du coronavirus COVID-19 a été déclarée;

op het Europese en internationale niveau, bepaalde opdrachten inzake gezondheid vervult, in het bijzonder wetenschappelijk onderzoek en risicobeoordeling;

• het bepaalt de categorieën van gegevens, zowel persoonsgegevens als niet-identificeerbare gegevens, die door de contactopsporingsapplicatie mogen worden verwerkt;

• het benadrukt de mogelijkheid voor een gebruiker van een contactopsporingsapplicatie om de controle over zijn gegevens te behouden en naar keuze gegevens geheel of gedeeltelijk te verwijderen;

• het benadrukt de nood aan transparantie en informatie aan de gebruiker van een contactopsporingsapplicatie;

• het bepaalt de bewaartermijnen die gelden voor de verzamelde gegevens;

• het waarborgt dat gegevens in een aparte loglijst of databank worden verzameld naargelang de doelstelling van de verwerking;

• het verbiedt de verwerking van de verzamelde gegevens voor andere doeleinden;

• het legt technische en organisatorische vereisten op voor de verwerkingsverantwoordelijke teneinde te waarborgen dat de verzamelde gegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging;

• het voorziet dat contactopsporingsapplicaties zelfuitdovend zijn teneinde te waarborgen dat geen gegevens meer worden verzameld zodra het einde van de toestand van de coronavirus COVID-19-epidemie wordt verklaard;

Kathleen VERHELST (Open Vld)
Michael FREILICH (N-VA)
Khalil AOUASTI (PS)
Jessika SOORS (Ecolo-Groen)
Gilles VANDEN BURRE (Ecolo-Groen)
Nathalie GILSON (MR)
Sammy MAHDI (CD&V)
Kris VERDUYCKT (sp.a)
Catherine FONCK (cdH)

PROPOSITION DE LOI

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

La présente loi prévoit la possibilité, dans le cadre des mesures de prévention de la propagation du coronavirus COVID-19 parmi la population, de permettre l'utilisation d'applications numériques de traçage de contacts pour les objectifs visés à l'art. 4, § 1.

La présente loi prévoit les fonctionnalités des applications numériques de traçage de contacts, les modalités et les conditions technologiques pour son utilisation, ainsi que les garanties de protection des droits et des libertés fondamentaux des citoyens.

Art. 3

Pour l'application de la présente loi, l'on entend par:

1° RGPD: Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

2° Loi Vie Privée: la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel;

Art. 4

§ 1er. Les applications numériques de traçage de contacts se limitent au traitement des informations permettant de:

— pouvoir confirmer une contamination COVID-19 d'un utilisateur d'une application numérique de traçage de contacts;

— prévenir les utilisateurs d'une application numérique de traçage de contacts que pendant un certain temps ils ont été à proximité d'une personne contaminée du COVID-19;

— effectuer des rechercher épidémiologiques sur la propagation du COVID-19 sur base de données anonymisées.

WETSVOORSTEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Deze wet voorziet in de mogelijkheid om, in het kader van de maatregelen ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking, het gebruik toe te laten van digitale contactopsporingsapplicaties voor de in art. 4, § 1 bepaalde doelstellingen.

Deze wet bepaalt de functionaliteiten van de digitale contactopsporingsapplicaties, de modaliteiten en technische voorwaarden voor het gebruik ervan alsook de waarborgen ter bescherming van de fundamentele rechten en vrijheden van de burgers.

Art. 3

Voor de toepassing van deze wet wordt verstaan onder:

1° AVG: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de richtlijn 95/46/EG;

2° Privacywet: de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

Art. 4

§ 1. De digitale contactopsporingsapplicaties beperken zich tot het verwerken van die informatie die moeten toelaten:

— een COVID-19-besmetting van een gebruiker van een digitale contactopsporingsapplicatie te kunnen bevestigen;

— de gebruikers van een digitale contactopsporingsapplicatie te verwittigen dat zij zich gedurende een bepaalde tijd in de nabijheid hebben bevonden van een met COVID-19 besmette persoon;

— epidemiologisch onderzoek uit te voeren betreffende de verspreiding van COVID-19 op basis van geanonimiseerde gegevens.

§ 2. A cet effet, les applications numériques de traçage de contacts doivent:

— générer une clé sécurisée ou plusieurs clés sécurisées dans l'équipement terminal de chaque utilisateur d'une application numérique de traçage de contacts afin de pouvoir générer des numéros de série temporaires non personnalisés;

— satisfaire aux exigences de l'interopérabilité afin de permettre la communication entre les appareils des utilisateurs ainsi qu'entre les appareils des utilisateurs et de la liste log visée à l'art. 8, § 1er;

— permettre la communication entre les appareils uniquement de manière anonymisée au moyen de numéros de séries temporaires non personnalisés basés sur une clé sécurisée propre à l'appareil de l'utilisateur;

— prévoir la possibilité d'échanger des clés avec d'autres pays qui utilisent le même système ainsi que le même niveau de garanties;

— prévoir la possibilité dans l'équipement terminal de l'utilisateur de relier les numéros de série temporaires non personnalisés sauvegardés avec les clés sécurisées qui sont sauvegardées dans la liste log visée à l'art. 8, § 1er;

— limiter les sauvegardes des informations dans les équipements terminaux des utilisateurs à des numéros de série temporaires non personnalisés, ainsi qu'un fuseau horaire comprenant une date et une partie de la journée de six heures dans laquelle un contact entre utilisateurs a eu lieu, ainsi que la distance et la durée de ce contact;

— permettre de manière anonymisée une authentification d'une application numérique de traçage de contacts;

— permettre à un utilisateur dont la contamination avec le COVID-19 a été constatée d'utiliser un code d'autorisation afin de copier dans ou transférer à la liste log visée à l'art. 8, § 1, la clé sécurisée ou les clés sécurisées ainsi que la date à laquelle l'utilisateur a été testé;

— garantir qu'uniquement les informations visées à l'art. 8, §§ 1er et 2 peuvent être communiquées au responsable du traitement;

— permettre aux utilisateurs d'éteindre temporairement l'application de traçage de contacts ainsi que d'effacer entièrement ou partiellement des informations sauvegardées dans leurs équipements terminaux;

§ 2. De digitale contactopsporingsapplicaties dienen daartoe:

— in de eindapparatuur van elke gebruiker van een digitale contactopsporingsapplicatie een beveiligde sleutel of een aantal beveiligde sleutels te genereren teneinde tijdelijke niet-gepersonaliseerde serienummers te kunnen genereren;

— te voldoen aan de vereisten van interoperabiliteit teneinde communicatie toe te laten tussen de toestellen van de gebruikers alsook tussen de toestellen van de gebruikers en de loglijst bedoeld in art. 8, § 1;

— de communicatie tussen de toestellen enkel op geanonimiseerde wijze te laten plaatsvinden, aan de hand van tijdelijke niet-gepersonaliseerde serienummers gebaseerd op een beveiligde sleutel die eigen is aan het toestel van de gebruiker;

— de mogelijkheid te voorzien om sleutels uit te wisselen met andere landen die hetzelfde systeem gebruiken en hetzelfde niveau van waarborgen;

— de mogelijkheid te voorzien om de in de eindapparatuur van de gebruiker bewaarde tijdelijke niet-gepersonaliseerde serienummers in verband te brengen met de beveiligde sleutels die worden bewaard in de loglijst bedoeld in art. 8, § 1;

— het opslaan van informatie in de eindapparatuur van de gebruikers te beperken tot de tijdelijke niet-gepersonaliseerde serienummers alsook een tijdszone bestaande uit een datum en een dagdeel van 6 uur waarbinnen een contact tussen gebruikers heeft plaatsgevonden, alsook de afstand en de duur van het contact;

— op geanonimiseerde wijze een authenticatie van een digitale contactopsporingsapplicatie toe te laten;

— een gebruiker waarvan de besmetting met COVID-19 is vastgesteld toe te laten een autorisatiecode te gebruiken teneinde de beveiligde sleutel of sleutels alsook de datum waarop de gebruiker getest werd te kopiëren in of door te geven aan de loglijst bedoeld in art. 8, § 1;

— te waarborgen dat enkel de in art. 8, §§ 1 en 2 bepaalde informatie kan worden meegedeeld aan de verwerkingsverantwoordelijke;

— gebruikers toe te laten de contactopsporingsapplicatie tijdelijk uit te schakelen alsook in hun eindapparatuur bewaarde informatie geheel of gedeeltelijk te verwijderen;

— prévoir la possibilité d'être désactivées;

— prévoir que la désinstallation des applications ne soit pas plus difficile que leur installation.

§ 3. Des spécifications techniques auxquelles les applications numériques de traçage de contacts doivent satisfaire sont prévues sur le site du responsable du traitement.

Art. 5

L'installation, l'utilisation et la désinstallation d'une application numérique de traçage de contacts se fait uniquement sur base volontaire.

L'installation ou la non installation, l'utilisation ou la non utilisation et la désinstallation ou la non désinstallation d'une application numérique de traçage de contacts ne peut en aucun cas donner lieu à une mesure civile ou pénale, à quelconque action discriminatoire ou à quelconque avantage ou désavantage.

Art. 6

§ 1er. Le responsable du traitement dans le sens de l'art. 4, 7° du RGPD est l'organisme de recherche Sciensano.

§ 2. Au moment de l'installation d'une application numérique de traçage de contacts le responsable du traitement fournit à l'utilisateur les informations telles que déterminées à l'art. 13 du RGPD.

Art. 7

§ 1er. Les applications numériques de traçage de contacts traitent et conservent nécessairement les clés sécurisées, les numéros de série temporaires non personnalisés générés par les applications, un fuseau horaire comprenant une date et une partie de la journée de six heures dans laquelle un contact entre utilisateurs a eu lieu, ainsi que la distance et la durée de ce contact.

La distance, la durée et le moment exact de ce contact ne sont pas communiquées aux utilisateurs.

§ 2. L'utilisateur peut insérer volontairement les informations suivantes dans l'application numérique de traçage de contacts:

— la contamination de COVID-19 constatée;

— le numéro de téléphone de l'utilisateur.

— de mogelijkheid te voorzien om gedeactiveerd te kunnen worden;

— dat het de-installeren van de applicaties niet moeilijker is dan de installatie ervan.

§ 3. Op de website van de verwerkingsverantwoordelijke worden de technische specificaties vermeld waaraan de digitale contactopsporingsapplicaties moeten voldoen.

Art. 5

Het installeren, het gebruiken en het de-installeren van een digitale contactopsporingsapplicatie gebeurt uitsluitend op vrijwillige basis.

Het al dan niet installeren, het al dan niet gebruiken en het al dan niet de-installeren van een digitale contactopsporingsapplicatie kan geen aanleiding geven tot enige burgerrechtelijke of strafrechtelijke maatregel, tot enige discriminerende handeling of tot enig voordeel of nadeel.

Art. 6

§ 1. De verwerkingsverantwoordelijke in de zin van art. 4, 7° van de AVG is de onderzoeksinstelling Sciensano.

§ 2. Op het moment van het installeren van een contactopsporingsapplicatie verstrekt de verwerkingsverantwoordelijke aan de gebruiker de informatie zoals bepaald in art. 13 van de AVG.

Art. 7

§ 1. De digitale contactopsporingsapplicaties verwerken en bewaren noodzakelijk de beveiligde sleutels, de tijdelijke niet-gepersonaliseerde serienummers die door de applicaties worden gegenereerd, een tijdszone bestaande uit een datum en een dagdeel van 6 uur waarbinnen een contact tussen gebruikers heeft plaatsgevonden, alsook de afstand en de duur van het contact.

De afstand, de duur en het exacte tijdstip van contact worden niet gecommuniceerd aan de gebruikers.

§ 2. De gebruiker kan vrijwillig volgende informatie ingeven in de contactopsporingsapplicatie:

— de met COVID-19 vastgestelde besmetting;

— het telefoonnummer van de gebruiker.

§ 3. L'utilisateur peut insérer son numéro de téléphone dans l'application numérique de traçage de contacts au moment où l'utilisateur se trouve chez un prestataire de soins de santé pour un prélèvement de matériel qui constitue la base d'un test PCR, afin de valider le lien entre l'utilisateur et son appareil.

§ 4. Le moment exacte auquel le contact a eu lieu ainsi que l'endroit n'est en aucun cas enregistré.

§ 5. L'objectif visé à l'art. 4, § 1er, troisième point est optionnel. Lors de l'installation de l'application numérique de traçage de contacts l'utilisateur doit confirmer explicitement que les informations visées à l'art. 8, § 2 peuvent être communiquées au responsable du traitement.

Art. 8

§ 1er. Les informations suivantes sont communiquées à et sauvegardées dans une liste log centrale auprès du responsable du traitement pour les objectifs visés à l'art. 4, § 1er, premier et deuxième point:

— la clé sécurisée ou les clés sécurisées d'un utilisateur dont la contamination avec le COVID-19 a été constatée et ensuite validée au moyen d'un code d'autorisation;

— la date à laquelle l'utilisateur est présumé avoir été contaminé.

§ 2. Les informations suivantes peuvent être communiquées à et sauvegardées dans une banque de données centrale auprès du responsable du traitement pour l'objectif visés à l'art. 4, § 1er, troisième point:

— la contamination de COVID-19 constatée;

— pour chacune des personnes contaminée du COVID-19 avec qui l'utilisateur a été en contact: la clé sécurisée de la personne en question, le nombre de rencontres que l'utilisateur a eu avec cette personne et pour chacune des rencontres le nombre de jours depuis la date de contamination du COVID-19 de la personne en question où la date à laquelle la contamination a été constaté;

— le nombre de numéros de série uniques non personnalisées de personnes contaminées.

Ces informations doivent être conservées séparément de la liste log visée au premier paragraphe et ne peuvent aucunement être interconnectées.

§ 3. De gebruiker kan zijn telefoonnummer in de contactopsporingsapplicatie ingeven op het moment dat de gebruiker bij een zorgverstrekker is om materiaal te laten afnemen dat de basis vormt voor een PCR-test, teneinde de link tussen de gebruiker en zijn toestel te valideren.

§ 4. Het exacte tijdstip en de plaats waarop het contact plaats heeft gevonden worden in geen geval geregistreerd.

§ 5. De doelstelling bedoeld in art. 4, § 1, derde streepje is optioneel. Bij het installeren van de contactopsporingsapplicatie dient de gebruiker uitdrukkelijk te bevestigen dat de informatie bedoeld in art. 8, § 2 aan de verwerkingsverantwoordelijke kan worden meegedeeld.

Art. 8

§ 1. Volgende informatie wordt in een centrale loglijst meegedeeld aan en bewaard bij de verwerkingsverantwoordelijke voor de in art. 4, § 1, eerste en tweede streepje bepaalde doelstellingen:

— de beveiligde sleutel of sleutels van een gebruiker waarvan de besmetting met COVID-19 is vastgesteld en vervolgens gevalideerd aan de hand van een autorisatiecode;

— de datum waarop de gebruiker vermoedelijk besmet is geworden.

§ 2. Volgende informatie kan worden meegedeeld aan en bewaard in een centrale databank bij de verwerkingsverantwoordelijke voor de in art. 4, § 1, derde streepje bepaalde doelstelling:

— de met COVID-19 vastgestelde besmetting;

— voor elke met COVID-19 besmette persoon waarmee de gebruiker in contact is geweest: de beveiligde sleutel van die persoon, het aantal ontmoetingen die de gebruiker heeft gehad met die persoon en voor elke ontmoeting het aantal dagen sinds de datum waarop die persoon besmettelijk was of waarop de COVID-19-besmetting werd vastgesteld;

— het aantal unieke niet-gepersonaliseerde serienummers van besmette personen.

Deze informatie moet apart bewaard worden van de loglijst bedoeld in de eerste paragraaf en mag in geen geval met elkaar in verbinding worden gebracht.

Art. 9

§ 1er. Les clés sécurisées, les numéros de série temporaires non personnalisés, le fuseau horaire dans lequel un contact a eu lieu entre utilisateurs ainsi que la distance et la durée du contact doivent être effacés au plus tard trois semaines après être générés dans l'équipement final de l'utilisateur d'une application numérique de traçage de contacts.

Une fois que la clé sécurisée ou les clés sécurisées arrivent dans la liste log visée à l'art. 8, § 1er elles ne peuvent plus être utilisées par l'équipement terminal de l'utilisateur. Elles sont retirées de l'équipement terminal de l'utilisateur, une nouvelle clé sécurisée est générée et de nouveaux numéros de série temporaires non personnalisés sont calculés.

La contamination de COVID-19 constatée, ainsi que le numéro de téléphone, pour autant que ces informations sont traitées en application de l'art. 7, § 2, doivent être effacés immédiatement après qu'elles ont été insérées dans dans l'application numérique de traçage de contacts.

§ 2. Les informations conservées dans la liste log visée à l'art. 8, § 1 doivent être effacés au plus tard trois semaines après être repris dans la liste log.

§ 3. Les applications numériques de traçage de contacts sont désactivées par le responsable du traitement aussitôt que le jour de la publication de l'arrêté royal proclamant la fin de l'état d'épidémie du coronavirus COVID-19.

La désactivation des applications numériques de traçage de contacts ne doit pas dépendre de la désinstallation par l'utilisateur.

Art. 10

Nonobstant le deuxième alinéa du présent article, les informations collectées ne peuvent pas être utilisées à d'autres fins que celles visées à l'art. 4, § 1, en particulier mais pas exclusivement des objectifs de police, commerciaux, pénaux, ou liés à la sûreté de l'État.

Les informations collectées peuvent être traitées conformément aux conditions visées au Titre 4 de la Loi Vie Privée à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques visés à l'art. 89, §§ 2 et 3 du RGPD.

Art. 9

§ 1. De beveiligde sleutels, de tijdelijke niet-gepersonaliseerde serienummers, de tijdszone waarbinnen een contact tussen gebruikers heeft plaatsgevonden, alsook de afstand en de duur van het contract dienen te worden gewist ten laatste drie weken nadat ze zijn gegenereerd in de eindapparatuur van de gebruiker van een digitale contactopsporingsapplicatie.

Eens de beveiligde sleutel of sleutels terechtkomen in de loglijst bedoeld in art. 8, § 1 mogen zij niet meer gebruikt worden door de eindapparatuur van de gebruiker. Zij worden verwijderd uit de eindapparatuur van de gebruiker, er wordt een nieuwe beveiligde sleutel gegenereerd en er worden nieuwe tijdelijke niet-gepersonaliseerde serienummers berekend.

De met COVID-19 vastgestelde besmetting alsook het telefoonnummer, voor zover deze informatie in toepassing van art. 7, § 2 wordt verwerkt, moeten onmiddellijk gewist worden nadat ze in de contactopsporingsapplicatie ingegeven werden.

§ 2. De in de loglijst bedoeld in art. 8, § 1 bewaarde informatie dient te worden gewist ten laatste drie weken nadat ze in de loglijst werd opgenomen.

§ 3. De digitale contactopsporingsapplicaties worden onverwijld door de verwerkingsverantwoordelijke gedeactiveerd vanaf de dag van de publicatie van het koninklijk besluit dat het einde van de toestand van de coronavirus COVID-19 epidemie afkondigt.

Het deactiveren van de digitale contactopsporingsapplicaties mag niet afhankelijk zijn van de-installatie door de gebruiker.

Art. 10

Onverminderd het tweede lid van dit artikel mag de verzamelde informatie niet gebruikt worden voor andere dan de in art. 4, § 1 bepaalde doelstellingen, in het bijzonder maar niet uitsluitend politionele, commerciele, strafrechtelijke, of aan staatsveiligheid verbonden doelstellingen.

De verzamelde informatie mag overeenkomstig de voorwaarden bepaald in Titel 4 van de Privacywet verwerkt worden met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden bedoeld in art. 89, §§ 2 en 3 van de AVG.

Art. 11

§ 1er. Pour le traitement des informations reprises dans la liste log et la banque de données visées à l'art. 8, §§ 1er et 2, le responsable du traitement prévoit une gestion stricte et adéquate des accès et des utilisateurs qui permet d'identifier des utilisateurs, de les authentifier et de contrôler et gérer leurs caractéristiques ou qualités pertinentes, mandats et autorisations d'accès. A cet effet, le responsable du traitement utilise des techniques informatiques qui:

— garantissent l'origine de l'accès au moyen de techniques de sécurisation adaptées;

— garantissent la confidentialité de l'accès;

— permettent une identification univoque du bénéficiaire et de l'authentifier au moyen d'un module d'authentification de la carte d'identité électronique ou un système adéquat garantissant un niveau de sécurisation similaire et pour constater le moment de l'accès de manière univoque;

— enregistrent une preuve d'accès dans le système;

— enregistrent les informations suivantes dans le système: l'identité du bénéficiaire, la date et le moment de l'accès; les données d'identification de la personne sur laquelle on a demandé des consultations; le dossier qui a été accédé; les finalités de la consultation;

— rapportent des erreurs de système et enregistrent les moments où les erreurs de système ont empêché l'accès et rendent ces périodes systématiquement disponibles pour les intéressés.

Les informations enregistrées sont sauvegardés pendant 3 ans.

§ 2. Le responsable du traitement prévoit les mesures techniques et organisationnelles nécessaires afin de garantir que les informations conservées dans la liste log et la banque de données visées à l'art. 8, §§ 1er et 2 ne sont aucunement être interconnectées.

Art. 12

La présente loi entre en vigueur le jour de sa publication au *Moniteur belge.*

La présente loi est d'application jusqu'au jour de la publication de l'arrêté royal proclamant la fin de l'état d'épidémie du coronavirus COVID-19.

Art. 11

§ 1. Voor de verwerking van de informatie opgenomen in de loglijst en databank bedoeld in art. 8, §§ 1 en 2 voorziet de verwerkingsverantwoordelijke in een strikt en adequaat gebruikers- en toegangsbeheer dat toelaat gebruikers te identificeren, te authentificeren en hun relevante kenmerken of hoedanigheden, mandaten en toegangsmachtigingen te controleren en beheren. Daartoe gebruikt de verwerkingsverantwoordelijke informaticatechnieken die:

— de oorsprong van de toegang verzekeren door middel van aangepaste beveiligingstechnieken;

— de vertrouwelijkheid van de toegang waarborgen;

— toelaten om de toegangsgerechtigde ondubbelzinnig te identificeren en te authentificeren aan de hand van een authentificatiemodule van de elektronische identiteitskaart of een passend systeem dat een gelijkwaardig beveiligingsniveau waarborgt en om het tijdstip van toegang ondubbelzinnig vast te stellen;

— een bewijs van toegang registreren in het systeem;

— de volgende informatie registreren in het systeem: de identiteit van de toegangsgerechtigde, de datum en het tijdstip van de toegang; de identificatiegegevens van de persoon over wie de raadpleging werd gevraagd; het dossier waarin toegang wordt genomen; de finaliteiten van de raadpleging;

— systeemfouten melden en de tijdstippen registreren waarop systeemfouten de toegang verhinderen en deze periodes systematisch beschikbaar maken voor de belanghebbenden.

De geregistreerde informatie wordt bewaard gedurende 3 jaar.

§ 2. De verwerkingsverantwoordelijke voorziet in de nodige technische en organisatorische maatregelen teneinde te waarborgen dat de informatie bewaard in de loglijst en databank bedoeld in art. 8, §§ 1 en 2 in geen geval met elkaar in verbinding worden gebracht.

Art. 12

Deze wet treedt in werking op de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

Deze wet is van toepassing tot de dag van de publicatie van het koninklijk besluit dat het einde van de toestand van de coronavirus COVID-19-epidemie afkondigt.

En toute circonstance, il est prévu une évaluation six mois après l'entrée en vigueur de la présente loi. Cette évaluation porte aussi sur l'efficacité des mesures prises en vertu de la présente loi.

11 mai 2020

In elk geval wordt er voorzien in een evaluatie zes maanden na de inwerkingtreding van deze wet. Deze evaluatie heeft ook betrekking op de doeltreffendheid van de maatregelen die werden genomen krachtens deze wet.

11 mei 2020

Kathleen VERHELST (Open Vld)
Michael FREILICH (N-VA)
Khalil AOUASTI (PS)
Jessika SOORS (Ecolo-Groen)
Gilles VANDEN BURRE (Ecolo-Groen)
Nathalie GILSON (MR)
Sammy MAHDI (CD&V)
Kris VERDUYCKT (sp.a)
Catherine FONCK (cdH)

Imprimerie centrale – Centrale drukkerij